

**UNITED STATES DISTRICT COURT  
DISTRICT OF NEW HAMPSHIRE**

**IN THE MATTER OF THE SEARCH OF  
184 HIGH STREET, SOMERSWORTH, NH**

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Shawn Serra, a Special Agent with the United States Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations, being duly sworn, do depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant relating to Joseph Gaudreau (hereafter “GAUDREAU”), who is the target of an ongoing investigation into possession and distribution of child pornography, and who lives in Somersworth, NH. The search warrant in support of which this affidavit is being submitted is for (1) the premises located 184 High Street, Somersworth, NH (hereafter “SUBJECT PREMISES”), further described in the respective Attachment A, including the residential dwelling, and (2) the person of GAUDREAU. The search warrants, as described more fully below and in the respective Attachment B, seek authority to search for and to seize computers, electronic devices capable of processing or storing electronic media, computer media, and other electronic media, located at and/or on the SUBJECT PREMISES, and the person of GAUDREAU, for the things described in the respective Attachment B – specifically, evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 2252(a)(4)(B), the illegal possession of child pornography.

2. I have been employed as an HSI Special Agent since June 2005, and am currently assigned to the Manchester, New Hampshire Resident Office. I graduated from the University of Massachusetts, Lowell, Massachusetts with a Bachelor of Science Degree in Criminal Justice. In 2003, I graduated from the University of Massachusetts, Lowell, Massachusetts with a Master of Arts Degree in Criminal Justice. I have also received training in the areas of child sexual exploitation, including violations pertaining to possession and production of child pornography, by attending a twenty-three-week training program at the Federal Law Enforcement Training Center (FLETC) in Glynco, Georgia. As part of my duties, I have observed and reviewed examples of child pornography (as defined in 18 U.S.C. § 2256) in various forms of media, to include digital/computer media. During the course of this investigation, I have also conferred with other investigators who specialize in computer forensics and who have conducted numerous investigations which involved child sexual exploitation offenses.

3. I am a “Federal law enforcement officer” within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant.

4. The information contained in this affidavit is based on information conveyed to me by other law enforcement officials, and my review of records, documents and other physical evidence obtained during this investigation. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have set forth all material information but have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of the Specified Federal Offenses are presently located on the Devices.

5. Based on my training and experience and the facts as set forth in this affidavit, I submit that there is probable cause to believe, and I do believe, that violations of 18 U.S.C. § 2252(a)(4)(B) (possession of child pornography) have occurred. There is also probable cause to search the premises, person, and devices described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

### **JURISDICTION**

6. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

### **PROBABLE CAUSE**

7. 18 U.S.C. § 2252 prohibits a person from knowingly possessing or accessing sexually explicit images (child pornography) with the intent to view them, as well as transporting, receiving, distributing or possessing in interstate or foreign commerce, or by using any facility or means of interstate or foreign commerce, any visual depiction of minors engaging in sexually explicit conduct (i.e., child pornography). The following definitions apply to this Affidavit and Attachment B:

- a. **“Child Exploitation Material”**, as used herein, includes known or identified victims depicted in a non-sexually explicit manner (various stages of undress, from the back, face only, etc.), and non-nude minors (clothed in sexually provocative poses, wearing sexually suggestive clothing or lingerie, etc.), of

indeterminate age (post-pubescent, sexually explicit, but unable to say for certain that they are under 18 years of age). **“Child Pornography”**, as used here, is defined in Title 18 United States Code § 2256 as any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

- b. **“Minor”** means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).
- c. **“Sexually explicit conduct”** means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

### **PROBABLE CAUSE**

8. On August 30, 2017, the New Hampshire Internet Crimes Against Children (ICAC) Task Force, executed a state search warrant for possession of child pornography at the SUBJECT PREMISES. During the course of the search warrant, GAUDREAU admitted to having child pornography on his cell phone and in a Dropbox account.

9. Based on the results of the search warrant and GAUDREAU's statements, the New Hampshire State Police obtained an arrest warrant for 3 counts of Possession of Child of Child Sexual Abuse Images. GAUDREAU turned himself in on November 4, 2017.

10. On April 3, 2019, the grand jury for the District of New Hampshire returned an indictment against GAUDREAU charging him with one count of Distribution of Child Pornography, in violation of 18 U.S.C. §§ 2252(a)(2), and one count of Possession of Child Pornography, in violation of 18 U.S.C. § 2252(a)(4)(B). GAUDREAU was arrested on April 15, 2019, and was released on conditions of supervision pending trial, including that he inform the court, defense counsel, and the U.S. Attorney's office in writing before any change in address or phone number. The current trial date is July 21, 2020.

11. On April 15, 2020, the NH ICAC received Cybertip 66061489 from the National Center for Missing and Exploited Children (NCMEC). In the Cybertip, the chat application Discord Inc. reported that on March 17, 2020, at 12:42 A.M.,<sup>1</sup> two files of suspected child pornography were uploaded by Screen/Username "fapmap34098#2141." Filename "iOS\_image\_upload\_9.jpeg" and filename "qny5vqz4gswc0iedndta.jpg" were uploaded from Internet Protocol Address (IP address) 70.20.57.7. The email address associated with the account was [openelligroup@gmail.com](mailto:openelligroup@gmail.com). The Cybertip also reported Discord Inc. had viewed the image.

12. Filename "iOS\_image\_upload\_9.jpeg" depicts a naked adult female lying next to a naked prepubescent female with her legs spread. The adult female's right hand is spreading the genitals of the prepubescent female. The prepubescent female's genitals are the focal point of

---

<sup>1</sup> The times discussed in this affidavit were originally provided in UTC but investigators converted them to EDT/EST for ease of reference.

the image. The female is clearly prepubescent because of her lack of breast development and pubic hair, and body structure.

13. Filename “qny5vqz4gswc0iedndta.jpg” depicts a prepubescent female, naked from the waist down, lying on her back in an upright position, with her legs spread exposing her genitals and anus. Her genitals are the focal point of the image. The female is clearly prepubescent because of her lack of pubic hair and body structure.

14. The IP address associated with the Cybertip geolocated to Dover, NH. Accordingly, the Cybertip was forwarded to the Dover Police Department. Detective (Det.) Adam Gaudreault requested that the Strafford County Attorney’s Office issue a subpoena for subscriber information for the IP address. On April 21, the Strafford County Attorney’s Office served the Internet Service Provider, Consolidated Communications with a subpoena for the IP address. On April 23, Consolidated Communications provided the following subscriber information: [REDACTED], 184 High Street, Somersworth, NH, 03878.

15. On April 23, 2020, the NH ICAC received Cybertip 66470390 from the NCMEC. In this Cybertip, the Discord Inc. reported that on March 22, 2020, at 11:40:32 P.M, username “fapallday#4904” uploaded two images believed to be child pornography. The email address associated with the account was “jaybruton02@gmail.com.” The images, bearing file names “iOS\_image\_upload\_11.jpeg” and “iOS\_image\_upload\_17.jpeg,” were uploaded from IP address 70.20.57.7. Discord Inc. indicated they had viewed the images.

16. Filename “iOS\_image\_upload\_11.jpeg” depicts a naked prepubescent female lying on her back with her legs spread exposing her genitals and anus. The prepubescent female is sucking the index finger of a woman on one side of her and has a naked adult female on the other side of her touching her genitals. The focal point of the image is the prepubescent female’s

genitals and anus. The female is clearly prepubescent because of her lack of breast development and pubic hair, and body structure.

17. Filename “iOS\_image\_upload\_17.jpeg” depicts a prepubescent female, naked from the waist down, lying on her back in between an adult male’s legs with his genitals removed from his pants. The female’s legs are in the air towards her face exposing her genitals and anus. The focal point of the image is the female’s anus and genitals. The female is clearly prepubescent because of her lack of pubic hair and body structure.

18. On May 6, 2020, the NH ICAC received Cybertip 69446941 from the NCMEC. In this Cybertip, the chat application Snapchat reported that screenname “jfoldarius1776” uploaded an image, filename “506be2d5-89ed-4456-a9d2-aa1a7804cd36\_CHAT\_MEDIA\_1587049378741.jpeg” believed to be child pornography. Snapchat reported the incident date and time as April 16, 2020, at 8:52 P.M, but did not provide an IP address. Snapchat listed July 29, 2019, 11:26 P.M. and IP Address 70.20.57.158 in the suspect portion of the Cybertip. Additional subscriber information provided in the Cybertip included a date of birth listed as August 5, 1995 and phone number (603) 866-1859. I note that the date of birth listed in the suspect portion is GAUDREAU’s birth date.

19. Filename “506be2d5-89ed-4456-a9d2-aa1a7804cd36\_CHAT\_MEDIA\_1587049378741.jpeg” depicts a prepubescent female, naked from the waist down, lying on her back with her legs spread exposing her genitals. Her legs are bent at the knees and she is manipulating an adult penis with her feet. The focal point of the image is the male’s genitals. The female is clearly prepubescent because of her lack of pubic hair and body structure.

20. On May 7, 2020, at the request of Det. Gaudreault, the Strafford County Attorney's Office served Consolidated Communications with a subpoena for subscriber information for IP address 70.20.57.158 on July 29, 2019, 11:26 P.M. On May 29, 2020, Consolidated Communications provided the following subscriber information: [REDACTED], 184 High Street, Somersworth, NH, 03878.

21. On June 8, 2020, I reviewed the three Cybertips and 5 associated images and determined the images to be child pornography.

22. According to U.S. Probation Officer Scott Davidson, who is supervising GAUDREAU on pretrial release, GAUDREAU lives at 184 High Street, Somersworth, New Hampshire, and has not changed his address after being released pending trial on April 15, 2019.

**CHARACTERISTICS COMMON TO INDIVIDUALS WHO DISTRIBUTE, RECEIVE, POSSESS, AND/OR ACCESS WITH INTENT TO VIEW CHILD PORNOGRAPHY**

23. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who distribute, receive, possess, and/or access with intent to view child pornography:

24. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

25. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of



children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

26. Such individuals almost always possess and maintain their hard copies of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home, storage spaces over which they have control, or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

27. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

28. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.

29. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography

distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

30. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. Thus, even if GAUDREAU uses a portable device (such as a mobile phone) to access the internet and child pornography, it is more likely than not that evidence of this access will be found in his home, the Subject Premises, in vehicles that he uses, and/or on the person of GAUDREAU, as set forth in Attachment A.

31. I believe that there is probable cause to believe violations of Title 18, United States Code, Section 2252(a)(4)(B), the illegal possession of child pornography will be found in the Subject Premises because GAUDREAU is the subject of an ongoing criminal case involving child pornography and the Cybertips indicate that activity has resumed at the SUBJECT PREMISES.

#### **BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET**

32. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

33. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

34. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

35. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types – to include computer hard drives, external hard drives, CDs, DVDs, and “thumb,” “jump,” or “flash” drives, which are very small devices which are plugged into a port on the computer – can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

36. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

37. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide e-mail services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as “cloud” storage) from any

computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone or external media in most cases.

### **SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS**

38. As described above and in Attachment B, this application seeks permission to search for records that might be found on the Subject Premises, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

39. I submit that if a computer or storage medium is found on the Subject Premises, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

40. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

41. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating

system may also keep a record of deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

42. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described in the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the Subject Premises because:

43. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

44. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and

experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpatng or exculpatng the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user’s

state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

45. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

46. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

47. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

48. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is

an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

49. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to “cloud” storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

50. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software website, or operating system that is being searched;

51. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover “hidden,” erased,



compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

52. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

53. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

54. Additionally, based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that routers,

modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of so-called "wireless routers," which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be "secured" (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or "unsecured" (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

55. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

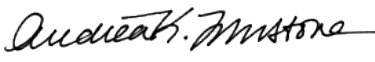
**CONCLUSION**

1. Based on the foregoing, there is probable cause to believe that the federal criminal statute cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of one or more of these offenses, more fully described in Attachment B, are located at the locations described in Attachment A. I respectfully request that this Court issue a search warrant for the locations described in Attachment A, authorizing the seizure and search of the items described in Attachment B.

/s/ Shawn Serra  
Special Agent Shawn Serra  
Department of Homeland Security  
Homeland Security Investigations

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. Crim. P. 4.1 and affirmed under oath the content of this affidavit and application.

Date: June 22, 2020  
Time: 9:15 AM



\_\_\_\_\_  
Andrea K. Johnstone  
U.S. Magistrate Judge



## **ATTACHMENT A**

### **DESCRIPTION OF LOCATIONS TO BE SEARCHED**

The entire property and residential building located at 184 High Street, Somersworth, New Hampshire, including the residential building. The residence of 184 High Street, Somersworth, New Hampshire is a three-story, white and gray home with a partial wrap around porch in the front extending to the right of the home. The residence is clearly marked with “184 High Street” immediately next to the front door. There is a dirt driveway to the left of the home as you face the front door with a side porch and bulkhead.







**ATTACHMENT A (continued)**

The person to be searched is Joseph GAUDREAU. GAUDREAU is a 24-year-old white male, five feet and six inches tall, with brown hair and green eyes.



**ATTACHMENT B**  
**ITEMS TO BE SEIZED**

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Section 2423 and violations of Title 18, United States Code, Section 2252:

1. Computers or storage media used as a means to commit the violations described above.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
  - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
  - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
  - c. evidence of the lack of such malicious software;
  - d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;

- e. evidence indicating the computer user's knowledge and/or intent as it relates to the crime(s) under investigation;
  - f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
  - g. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;
  - h. evidence of the times the COMPUTER was used;
  - i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
  - j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
  - k. records of or information about Internet Protocol addresses used by the COMPUTER;
  - l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and
  - m. contextual information necessary to understand the evidence described in this attachment.
- 3. Routers, modems, and network equipment used to connect computers to the Internet.
  - 4. Child pornography and child erotica.
  - 5. Records, information, and items relating to violations of the statutes described above including:



- a. Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;
- b. Records and information relating to the identity or location of the persons suspected of violating the statutes described above;
- c. Records and information relating to the sexual exploitation of children, including correspondence and communications between users of Discord and Snapchat;
- d. Records and information showing access to and/or use of Discord and Snapchat;

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.